

BioStation T2 is the IP network-based premium fingerprint verification terminal that delivers various authentication modes such as fingerprint, RFID, and PIN authentication for access control and time & attendance.

### Features

5 inch touchscreen LCD	R	An intuitive GUI provided on the high-durable 5 inch touchscreen LCD delivers easy user management and displays various information and notices.
Camera for face image capture	O.	The built-in high-performance camera detects the face image and captures image logs which delivers enhance security through valid identification check.
Embedded Web Server	<b>d Web</b> <b>er</b> The embedded web server (BioStar Lite) allows administrators to manage users and devices through a web browser in any PC without S/W and database installation.	
Fast matching speed	CPU	Loaded with world's best performing Suprema fingerprint algorithm and powerful dual CPU achieves unparalleled 1:3,000 fingerprint matches in less than a second.
Versatile Interfaces		Provides various interfaces, such as PoE, WiFi, TCP/IP, and RS485/232, allowing users to connect to PCs and configure the network. In addition, Wiegand and I/O ports allow users to configure various access control systems.
Video Phone	Video Phone         Provides IP-based AV interface and analog video phone functions.	
RF Card Options	Card	Supports EM, Mifare Classic, Mifare Plus, and Mifare DesFire(CSN) cards.

These safety instructions provided here are meant to guard your safety and prevent any possible damage or loss of property. Please carefully read these and keep them in mind when you use Suprema's product.

## **Safety Instructions**



Do not install the terminal in a place affected by direct sunlight, humidity, dust, or soot.



Keep the terminal away from magnets or anything containing magnetic material, such as magnet, TV sets, computer monitor (especially CRT) and speakers.



Keep the terminal away from any heating devices or heat sources.



Do not spill any liquids such as soda, water, or solutions into the terminal.



Use a soft cloth or towel when cleaning the terminal. Do not spray water on the terminal.



Clean the terminal regularly to prevent dust from settling onto it.



Do not drop the terminal or cause any impact on the terminal.



Do not apply heavy pressure to the touch screen.



Do not disassemble, repair, or reconstruct the terminal without any direction of Suprema. Otherwise, you cannot receive proper A/S for the terminal from Suprema.



Keep the product out of reach from children for safety purposes.



Do not use the terminal for any other purpose than its original use.



In case of product malfunction or problems, please contact Suprema's Customer Service Center or the sales agent.

#### **Table of Contents**

Before	e Getting Started	6
Comp	oonents	7
E E	Basic Components	7
	Optional Accessories	8
Name	es and Functions of Parts	9
I F	Front	9
E E	Bottom	10
F F	Rear	10
Dime	nsions	11
Menu	Screen	12
Stand	lby Screen	13
Authe	ntication Mode	14
How t	o place a finger	15

2 Installation	17
Installation	18
Connector/Cable Specifications	19
232 CABLE (3-pin Connector)	19
SWITCH CABLE (8-pin Connector)	19
RELAY CABLE (3-pin Connector)	20
WIEGAND CABLE (5-pin Connector)	20
POWER CABLE (2-pin Connector)	20
■ VIDEO PHONE CABLE (7-pin Connector)	21

RS485 CABLE (4-pin Connector)	21
Connection	22
Power Connection (2-pin Connector)	22
■ USB Cable Connection	23
Ethernet Connection (Ethernet Cable)	24
Ethernet Connection (Direct connection to PC)	25
PoE hub connection	26
■ Wireless Connection	27
■ USB Memory Connection	28
■ RS485 PC Connection (4-pin Connector)	29
■ RS485 Connection to Secure I/O	
or Other Terminals (4-pin Connector)	30
■ RS232 Connection	31
Videophone Connection	32
Relay Connection - Fail Safe Lock (3-pin Connector)	33
Relay Connection - Fail Secure Lock (3-pin Connector)	33
Relay Connection – Automatic Door (3-pin Connector)	34
■ TTL Switch Input Connection (8-pin Connector)	35
Wiegand Input (5-pin Connector)	36
Wiegand Output (5-pin Connector)	36
System Configuration	37
Standalone	37
Secured	37
Network Configuration	38

3 User Menu	39
Access Authentication	40
Fingerprint Authentication	40
Fingerprint Only	40
Fingerprint + Pin Authentication	40
T&A Key+Fingerprint Authentication	41
T&A Key + Fingerprint + Pin Authentication	41
Card Authentication	41
Card Only Authentication	41
Card + Password Authentication	42
Card + Fingerprint Authentication	42
Card + Fingerprint/Password Authentication	43
Card + Fingerprint + Password Authentication	43
ID Authentication	44
■ ID + Password Authentication	44
ID + Fingerprint Authentication	44
ID + Fingerprint/Password Authentication	45
■ ID + Fingerprint + Password Authentication	45
T&A Mode	46
■ T&A Mode Setup	46
T&A Authenticate Methods	47
■ T&A Event	47
Personal Entrance/T&A Record Check	47
Authentication Failures	48

4 Admin Menu	49
Registering an Admin	50
Entering into Admin Menu	51
Configuration of Admin Menu	52
User Enrollment process	54
Registering User to Device (using CSN)	55
Enroll User	56
Edit/Delete User	59
Search User	60
Checking the Registered User Info	61
Deleting All Users	61
Registering a User to a Card (using Template Card)	62
■ Issuing a Card	62
Formatting a Card	63
Network Setup	64
■ TCP/IP Setup	64
Server Setup	65
Serial Communication	65
USB	66
USB Memory	66
■ Wireless LAN	67
Authentication Mode	68
■ Finger Auth Mode	68
Card Auth Mode	68
■ ID Auth Mode	69

.

Operation
T&A Mode
■ T&A Event71
Camera Event71
Device Setup72
■ Fingerprint Setting
Door
Interphone Setting
■ Date & Time Setup75
Device Info
Memory Info75
Touchscreen Calibration
Touchkeypad Calibration
■ Reset
Factory Default
Display Setup77
Log78
■ Log List
Log Search
Delete All Log
Log Info79
5 Appendix
Product Specifications81
Electrical Specification82

HTTP://WWW.SUPREMAINC.COM

## BEFORE GETTING STARTED

Please check the package and ensure that all of the components are prepared.

### Components

#### Basic Components





**BioStation T2 Body** 





Mini USB Cable



Software CD (1 copy)



Screws and PVC Anchors (4 EA each)



Ferrite Core



Cables (7 types, 9 EA)

1 BEFORE GETTING STARTED

#### Optional Accessories



**Note** The product shown above is just an image to illustrate the product. Depending on Suprema's internal changes, some of the components shown here may be different and changed from the components that you have received.

### Names and Functions of Parts



No.	Name	Function	
1	Microphone	Used for interphone call.	
2	Proximity Sensor	A sensor that detects objects around the device without any physical contact. To reduce power consumption, BioStation T2 lowers the brightness of the backlight when no input is made for a specified time.	
3	Camera	Used for still image logs and video interphone.	
4	Card reader	Reads a RF card.	
5	Fingerprint Sensor LED	Displays the status of the fingerprint sensor. 1)ON – Waiting for fingerprint input 2)Blinking – Requesting for a specific fingerprint or fingerprint for registration	
6	Speaker	Outputs sound effects and voices.	
7	Fingerprint Sensor	Used to register and authenticate a user's fingerprint.	
8	CALL Key	Used to make a call when a video phone is connected.	
9	T&A Keys (F1~F4)	Used as function keys to select the T&A event	
10	Color LCD Screen	Displays time, status, and UI for operation.	



No.	Name	Function
1	USB type A	A slot to connect a USB memory
2 Mini USB		A slot to connect a PC to a USB.

Rear

No.	Name	Function
1	USB Wireless LAN port	A slot to connect the USB wireless LAN device. For the wireless LAN-supported BioStation T2 model, the wireless LAN device is mounted before released from the factory.
2	RJ45 Socket	Connects Ethernet cable
3, 4	3-pin Connector	Connects RELAY(0,1)
5, 6	4-pin Connector	Connects RS485(0,1)
7, 8	Termination Switch	RS485 TERMINATION Enable/Disable
9	8-pin Connector	SWITCH Input
10	3-pin Connector	Connects RS232 port
11	7-pin Connector	Connects VIDEOPHONE
12	5-pin Connector	WIEGAND Input/Output
13	2-pin Connector	Connects power supply
14	Slot for Micro SD Memory Card	Used to insert Micro SD-type memory card for extended functions.

1 BEFORE GETTING STARTED

### Dimensions

#### 155mm(W) x 155mm(H) x 40mm(D)



### Menu Screen



- 1 Status Bar: Displays the current date, time, and status icons.
- 2 ID: Enters the user ID for authentication.
- 3 T&A: Enters the additional T&A events.
- 4 Menu: Enters the administrator menu.
- 5 T&A Key Display: Describes operations of F1~F4, CALL keys. The buttons work like F1~F4, CALL keys.



 1
 ▲
 ↓
 ↓

 2
 ↓
 ↓
 ↓

 3
 ↓
 ↓
 ↓

 4
 ♥
 ♥
 ♥

Displays whether or not to use face detection option for image logs.

Displays Ethernet connection status and wireless LAN connection status.

Displays connection to PC via Ethernet and wireless LAN.

Displays RS485 connection.

### **Standby Screen**

#### Start-up Screen



	When time is hidden from the center of the screen for
lote	Theme 1 and Theme 3, the moving background
	screen is displayed.

#### **T&A Configuration**



The T&A event is displayed under the status bar.

#### Setting the Background Screen



Other Standby Screens



**Locked:** You can lock the terminal using the tampers position or a specific input port. To unlock the terminal, administrator's authentication is required.



**Armed:** When a security area is set, you can change the mode of the terminal to the security mode. To release the security mode, authentication by a user who belongs to the corresponding security group is required. For more details, see the BioStar manual.

### **Authentication Mode**

#### BioStation T2 supports various authentication modes using fingerprints, RFID card, and ID (PIN).

Fingerprint Authentication Mode	Card Authentication Mode	ID Authentication Mode
<ul> <li>Finger:</li> <li>Only fingerprints are used for authentication.</li> <li>Finger+Pin:</li> <li>For authentication, input the fingerprint and then type the password.</li> </ul>	<ul> <li>Card Only: Only a RF card is used for authentication.</li> <li>Card+Pin: For authentication, place the registered card onto the card reader and then type the password.</li> <li>Card+Finger: For authentication, place the registered card onto the card reader and then input the fingerprint.</li> <li>Card+Fnger/Pin: For authentication, place the registered card onto the card reader and then input the fingerprint.</li> <li>Card+Fnger/Pin: For authentication, place the registered card onto the card reader and then input the fingerprint or type the password.</li> <li>Card+Finger+Pin: For authentication, place the registered card onto the card reader, and then input the fingerprint and type the password.</li> </ul>	<ul> <li>ID+Pin:</li> <li>For authentication, type the registered ID and then type the password.</li> <li>ID+Finger:</li> <li>For authentication, type the registered ID and then input the fingerprint.</li> <li>ID+Finger/Pin:</li> <li>For authentication, type the registered ID and then input the fingerprint or type the password.</li> <li>ID+Finger+Pin:</li> <li>For authentication, type the registered ID, and then input the fingerprint and type the password.</li> </ul>

**Note** For more detailed description on each authentication mode, see [Chapter 3, User Menu > Access Authentication (p.40)].

### How to place a finger

#### Select a finger to enroll



(1) It is recommended to use an index finger or a middle finger.(2) Thumb, ring or little finger is relatively more difficult to place in a correct position.

#### How to place a finger on a sensor

(1) Place a finger as it completely covers the sensor with maximum contact.

(2) It is better to place the core part of a fingerprint to the center of a sensor.

- People usually tend to place only the top end of a finger
- Where is the core (center) of a fingerprint?
  - A peak where spirals of fingerprint ridges are dense
  - Usually opposite to lower part of a nail
  - It is recommended to place a finger as the lower part of a nail is located at the center of a sensor

(3) If a finger is placed as in the right picture, only a small area of a finger is captured. So it is recommended to place a finger as in the left picture.



Right



Wrong

#### Tips for different finger conditions

Suprema's fingerprint products are designed to scan fingerprint smoothly regardless of the conditions of a finger skin. However, if a fingerprint is difficult to scan due to other influences, please refer to the followings tips.

(1) If a finger is stained with sweat or water, scan after wiping moisture off.

(2) If a finger is covered with dust or impurities, scan after wiping them off.

(3) If a finger is way too dry, scan after blowing warm breath on a fingertip.

#### Advices on fingerprint enrollment

(1) In fingerprint recognition, enrollment process is very important. Therefore, when enrolling a fingerprint, please try to place a finger correctly with care.

(2) In case of low acceptance ratio, the following actions are recommended.

- Delete enrolled fingerprints and re-enroll the fingers.
- Enroll the same finger additionally
- Try with another finger if a finger is not easy to enroll due to scar or worn-out.

(3) For the case when an enrolled fingerprint can't be used due to scar or holding a baggage, it is recommended to enroll more than two fingers.

HTTP://WWW.SUPREMAINC.COM

# **2** INSTALLATION

#### 2 INSTALLATION

### Installation

BioStation T2 has a camera for face detection and video interphone. Therefore, height of the product and its camera angle are very important factors in installation. For easy face detection and fingerprint authentication, determine the place where the product should be installed. We recommend you to install the product at the height of 130 cm  $\sim$  140 cm from the floor and the minimum distance between the product and the human is 40 cm.





1. Adjust the wall mounted bracket to the desired place on the wall and then fix it firmly to the wall.



2. Attach the product on the fixed wall mounted bracket and fix it to the bracket using the screw located at the bottom of the wall mounted bracket.

### **Connector/Cable Specifications**

#### 232 CABLE (3-pin Connector)

Pin	Name	Cable Type	Color
1	232RX		GREEN
2	232TX	AWG26	YELLOW
3	GND		BLACK



#### SWITCH CABLE (8-pin Connector)

Pin	Name	Cable Type	Color
1	SWITCH INPUT0		YELLOW
2	SWITCH INPUT1		GREEN
3	SWITCH GND		BLACK
4	SHIELD GND		GRAY
5	SWITCH INPUT2	AWG20	WHITE
6	SWITCH INPUT3		ORANGE
7	SWITCH GND		BLACK
8	SHIELD GND		GRAY



2 INSTALLATION

#### RELAY CABLE (3-pin Connector)

Pin	Name	Cable Type	Color
1	RELAY NORMAL OPEN		WHITE
2	RELAY COMMON	AWG24	BLUE
3	RELAY NORMAL CLOSE		ORANGE



#### WIEGAND CABLE (5-pin Connector)

Pin	Name	Cable Type	Color
1	DATA0		GREEN
2	DATA1		WHITE
3	GND	AVVG20	BLACK
4	SHIELD GND		GRAY



#### POWER CABLE (2-pin Connector)

Pin	Name	Cable Type	Color
1	POW +	ANA/0.04	RED
2	POW -	AWG24	BLACK



2 INSTALLATION

#### ■ VIDEO PHONE CABLE (7-pin Connector)

Pin	Name	Cable Type	Color
1	VOICE SIGNAL		RED
2	GND		BLUE
3	POWER		YELLOW
4	VIDEO SIGNAL	AWG26	WHITE
5	DOOR OPEN SIGNAL		ORANGE
6	GND		BLACK
7	SHIELD GND		GRAY



#### RS485 CABLE (4-pin Connector)

Pin	Name	Cable Type	Color
1	RS485 TRX+		BLUE
2	RS485 TRX-		YELLOW
3	GND	AWG20	BLACK
4	SHIELD GND		GRAY



### Connection

#### Power Connection (2-pin Connector)



- **Note** You should use a 12V adapter which is covered by IEC/EN 60950-1, providing voltage of 12V±10% and a current of 1500mA or above.
  - It is recommended that the power of BioStation T2 shall not be shared with other devices such as Secure I/O and Lock.

2 INSTALLATION

#### USB Cable Connection



#### Ethernet Connection (Ethernet Cable)

Connect the RJ45 socket on the rear of the product to the hub with an Ethernet (LAN) cable.



#### Ethernet Connection (Direct connection to PC)



#### PoE hub connection

PoE (Power over Ethernet) is an Ethernet connection of which power is provided by IEEE802.3af standard-compliant PSE (Power sourcing Equipment).



**Note** *If you use PoE, the length of a LAN cable should be within 100 m.* 

#### Wireless Connection

Wireless connection is made by mounting the USB wireless LAN module. For the wireless LAN-supported BioStation T2, the wireless LAN device is mounted before released from the factory.



The performance of a wireless LAN depends on the type of the AP (access point) and the environment.
 Some wireless APs will not be fully compatible with the terminal so that the wireless LAN connection may not be successful.
 The wireless APs listed below are fully compatible with the BioStation T2.

- Buffalo WHR-HP-G54
- IP Time G104

2 INSTALLATION

#### USB Memory Connection

User data or log data can be downloaded/uploaded using a USB memory.



Some USB memories will not be fully compatible with the terminal so that the connection may not be successful. The USB memories listed below are fully compatible with the BioStation T2.

- [IMATION] Flash Drive Nano 4GB
- [LG Electronics] X TICK M4 4GB
- [LG Electronics] X TICK MOBY J1 2GB
- [PQI] Traveling Disk U173 4GB

Note

- [Samsung C&T Corporation] PLEOMAX PUB-S100 4GB
  - [IMATION] Flash Drive Nano 4GB
  - [LG Electronics] X TICK M4 4GB
  - [LG Electronics] X TICK MOBY J1 2GB
  - [PQI] Traveling Disk U173 4GB
  - [Samsung C&T Corporation] PLEOMAX PUB-S100 4GB

#### RS485 PC Connection (4-pin Connector)



Note	<i>If the RS485 cable is too long, the signal may be weakened. In this case, you should install a terminating resistance at both ends of the bus by turning on the Dip Switch for normal signal transmission On the other hand, if the cable is too short, the resistance may interrupt signal</i>
INOLE	transmission. Therefore, by considering the length of the cable and the signal status, select whether to turn on or off the terminating resistance switch.

**Caution!** - Only the devices at the both ends of the bus should be terminated.

- If you do not connect GND, the RS485 chip may be damaged or communication may not be successful.

#### RS485 Connection to Secure I/O or Other Terminals (4-pin Connector)



Note One RS485 network can be connected to 8 terminals in maximum, including a Host.

Caution! If you do not connect GND, the RS485 chip may be damaged or communication may not be successful.

2 INSTALLATION

#### RS232 Connection



2 INSTALLATION

#### Videophone Connection



	The only following videophone models are compatible with BioStation T2.
Note	<ul> <li>COMMAX / CAV-35N</li> <li>COMMAX / CAV-50H</li> <li>COMMAX / CAV-50P</li> </ul>

### (1) Normally Open / N.O (White) -(2) Common (Blue) (3) Normally Close /N.C (Orange) Deadbolt / DC Power supply

Relay Connection - Fail Secure Lock (3-pin Connector)

Relay Connection - Fail Safe Lock (3-pin Connector)



Note
 -Normally Open/N.O: When no control signal is received, the electricity does not flow. When control signals are received, the electricity continues flowing.
 -Normally Close/N.C: When no control signal is received, the electricity continues flowing. When control signals are received, the electricity does not flow.

#### Relay Connection – Automatic Door (3-pin Connector)



#### **TL Switch Input Connection (8-pin Connector)**


2 INSTALLATION

# Wiegand Input (5-pin Connector)



# Wiegand Output (5-pin Connector)



**Note** There is only one Wiegand port. Select either of Wiegand Output and Wiegand Input using BioStar software.

# **System Configuration**

# **Standalone**

A terminal works both of door control and authentication functions.



# Secured

A terminal works as authentication function. Secure I/O works as a door controller.



2 INSTALLATION

# Network Configuration

LAN and RS485 allow integrated management.



HTTP://WWW.SUPREMAINC.COM

# **3** USER MENU

3 USER MENU

# Access Authentication

BioStation T2 supports three authentication types: fingerprint, Card(RFID), and ID(PIN). The authentication modes are operated in accordance with the set time schedule and the time schedule of each authentication means is not overlapped with the others. Up to 128 of time schedules can be set through BioStar software.

# Fingerprint

### Fingerprint Only

<How to Set>

- 1. [Menu] > [Mode] > [Finger Auth Mode] > [Finger]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



Place a finger on the sensor.



The authentication success screen is then displayed only when the card authentication has succeeded.

- *If the user's picture has been registered: he user's picture is then displayed on the authentication success screen.*
- Note If the user's picture has not been registered: The recorded image is displayed. If the still image log has not been recorded, the default image is then displayed on the authentication success screen.

### Fingerprint + Pin Authentication

### <How to Set>

2

3

- 1. [Menu] > [Mode] > [Finger Auth Mode] > [Finger+Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



Place a finger on the sensor.

- A PIN number input window appears.
  - Enter the password(PIN number) and then press [OK].
- An authentication success screen is displayed.

#### 3 USER MENU

### ■ T&A Key+Fingerprint Authentication

<How to Set>

- 1. [Menu] > [Mode] > [Finger Auth Mode] > [T&A Key+Finger]
- 2. Select either of Always or the desired time schedule.

#### <How to Authenticate>

- 1 Press the desired T&A Key (F1~F4).
- 2 Place a finger on the sensor.
- 3 An authentication success screen is displayed.

### ■ T&A Key + Fingerprint + Pin Authentication

<How to Set>

- 1. [Menu] > [Mode] > [Finger Auth Mode] > [T&A Key+Finger+Pin]
- 2. Select either of Always or the desired time schedule.

#### <How to Authenticate>

- 1 Press the desired T&A Key (F1~F4).
- 2 Place a finger on the sensor.
- 3 A PIN number input window appears. Enter the password(PIN number) and then press [OK].
- 4 An authentication success screen is displayed.

# Card

### Card Only Authentication

Card Only authentication is enabled when the authentication mode is set to 'Card Only' status or the user's card has been registered as a Bypass card.

<How to Set>

- 1. [Menu] > [Mode] > [Card Auth Mode] > [Card Only]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



- Place the card into the card reader.
- 2 An authentication success screen is displayed.

### Card + Password Authentication

<How to Set>

- 1. [Menu] > [Mode] > [Card Auth Mode] > [Card+Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



- 1 Place the card into the card reader.
- 2 A PIN number input window appears. Enter the password(Pin number) and then press [OK].
- 3 An authentication success screen is displayed.

### Card + Fingerprint Authentication

<How to Set>

- 1. [Menu] > [Mode] > [Card Auth Mode] > [Card+Finger]
- 2. Select either of Always or the desired time schedule.

<How to Authenticate>



- 1 Place the card into the card reader.
- 2 A fingerprint input window appears, place a finger on the sensor.
- 3 An authentication success screen is displayed.

### Card + Fingerprint/Password Authentication

<How to Set>

- 1. [Menu] > [Mode] > [Card Auth Mode] > [Card+Finger/Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



- 1 Place the card into the card reader.
- 2 Input the fingerprint or type the password.
- 3 An authentication success screen is displayed.

# ■ Card + Fingerprint + Password Authentication <*How to Set>*

- 1. [Menu] > [Mode] > [Card Auth Mode] > [Card+Finger+Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



1





- Place the card into the card reader.
- 2 A fingerprint input window appears, place a finger on the sensor.
- 3 A PIN number input window appears. Enter the password(PIN number) and then press [OK].
- 4 An authentication success screen is displayed.

### 

### ■ ID + Password Authentication

<How to Set>

- 1. [Menu] > [Mode] > [ID Auth Mode] > [ID+Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



- 1 On the Standby Screen, press [ID].
- 2 An ID input window appears, Enter your ID.
- 3 A PIN number input window appears. Enter the password(PIN number) and then press [OK].
- 4 An authentication success screen is displayed.

### ■ ID + Fingerprint Authentication

<How to Set>

- 1. [Menu] > [Mode] > [ID Auth Mode] > [ID+Finger]
- 2. Select either of Always or the desired time schedule.

#### <How to Authenticate>



- On the Standby Screen, press [ID].
- 2 An ID input window appears, Enter your ID.
- 3 A fingerprint input window appears. Place the finger on the scanner.
- 4 An authentication success screen is displayed.

### ■ ID + Fingerprint/Password Authentication

<How to Set>

- 1. [Menu] > [Mode] > [ID Auth Mode] > [ID+Finger/Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



- 1 On the Standby Screen, press [ID].
- 2 An ID input window appears, Enter your ID.
- 3 An Authentication window appears. Enter the password or place the finger on the scanner.
- 4 An authentication success screen is displayed.

# ■ ID + Fingerprint + Password Authentication <How to Set>

- 1. [Menu] > [Mode] > [ID Auth Mode] > [ID+Finger+Pin]
- 2. Select either of Always or the desired time schedule.

### <How to Authenticate>



- 1 On the Standby Screen, press [ID].
- 2 An ID input window appears, Enter your ID.
- 3 A fingerprint input window appears, place a finger on the sensor.
- 4 A PIN number input window appears. Enter the password(PIN number) and then press [OK].
- 5 An authentication success screen is displayed.

# T&A Mode

# **T&A Mode Setup**

1 [Menu] > [Mode] > [T&A Mode]

2 Select a desired T&A mode.

### Manual(by key input)



If the T&A mode is set to [Manual], press the F1 to F4 key or the extended T&A key to select a predefined T&A event. The selected T&A event is released after authentication.

### Auto(by time schedule)



If the T&A mode is set to [Auto] mode, the predefined T&A event will be automatically applied in accordance with the specified time period which is set in BioStar. You can define T&A event and time period in BioStar. To change the current T&A event to another T&A event, press the T&A key to select the desired T&A event.

### Manual Fix(by key input)



If the T&A mode is set to [Manual Fix] mode, you can select a T&A event like [Manual]. Press the F1 to F4 key or the extended T&A key to select a predefined T&A event. However, different from [Manual] mode, the once selected T&A event is kept until another T&A event is selected in [Manual Fix].

### Fixed(by device)



If the T&A mode is set to [Fixed] mode, authentication is available only with the fixed T&A event. You cannot select any other T&A event but the fixed one. You can define a fixed T&A event in BioStar.

### Disabled



Select [Disabled] mode to use access authentication only without T&A management.

# T&A Authenticate Methods

- Press the F1 to F4 key or the corresponding T&A button on the screen and select a desired T&A event. (Ignore this step at [Auto] or [Fixed] mode)
- 2 Proceed with authentication procedures. (identical with that of access authentication)
- 3 An authentication success window is then displayed and the T&A event is applied.

# **T&A Event**

### Basic T&A Events (F1~F4)

#### от рм 02:02 | Status ▼



- There are four basic T&A events. To select one of those, press the T&A button at the bottom of the screen or the F1 to F4 keys.
- In: Arrive at work.
- Out: Leave after work.
- In Duty: Return during work.
- Out Duty: Leave temporarily during work.

### Additional T&A Event



You can select the additional T&A events, predefined by the BioStar software. To select the additional T&A event, press [T&A] button on the Start-up screen.

# Personal Entrance/T&A Record Check



You can check your entrance/T&A records. To check it, follow the procedures below.

- 1 On the Standby screen, select [Menu].
- 2 Place the finger or the card or press [ID] and enter the ID.
- 3 You can check your entrance/T&A records.

	The personal entrance/T&A record check is for the general
Note	users only. Administrators can enter into Admin Menu
	using the above procedures. (See p.51)

# **Authentication Failures**

Access denied	I Displayed when authentication is failed.
Auth Mode Error	I Displayed when the authentication mode does not match up.
Invalid time interval	I Displayed when authentication is limited by authentication interval limit.
Exceeded count	I Displayed when the number of authentications exceeds the specified authentication count.
Access is not granted	I Displayed when the user does not belong to the Access Group.
Anti-passback failed	Displayed when the access is limited by Anti-passback.
Unregistered User	I Displayed when the user is an unregistered user or the user information is not saved in the data card.

HTTP://WWW.SUPREMAINC.COM

# 4 ADMIN MENU

# **Registering an Admin**

There is no registered user data in the product delivered from the factory. Please register the administrator immediately after the first installation of BioStation T2. The Admin can add/delete users and configure terminal settings.



- 1 Select [Menu] > [User] > [Enroll User].
- 2 Enter the user ID and at least one of card information, password, and fingerprints.
- 3 Check the Admin Level checkbox and then press [Save] button.

User Info Items
Face
User ID
Name
Fingerprint
Card
Password
Administrator
Duress Finger
Bypass Card
Individual Auth
Access Group

**Note** The admin registration procedure is identical with that of user registration except the [Admin Level] checkbox. Please see the user registration pages. (p.55~p.58)

## Entering into Admin Menu



- 1 On the main screen, press [Menu].
- 2 The [Enter Admin menu] screen is displayed.
- 3 Place the card close to the card reader on the terminal or press [ID] and enter the ID.
- 4 If required, enter the password and click [OK].
- 5 The Admin Menu is displayed.

If no user has been registered and you press [Menu], you will enter into the Admin Menu without any authentication procedures.
The general user, not the administrator, enters into his/her entrance/T&A log check screen. (See p.47)

### Configuration of Admin Menu



4 ADMIN MENU



# **User Enrollment Process**



# <Using CSN Card>

3

# **Registering User to Device**

When a card reader recognizes a CSN card, it compares the unique identification number of the card to the unique identification number of the card registered to the device. The unique identification number is saved in the device when a user is registered to the device. To use the CSN card, select [Mode] > [Operation] > [Card Mode] and select [Use CSN]. The EM model supports CSN card authentication mode only.

Jun <sup>30</sup> Thu AM 07:58   Status ▼	Jun 30 Thu AM 07:58 Status •		un 30 Thu АМ 07:58	Status 🔻
Luser	Enroll User		Menu > User > Enroll User	
丘牙 Network	Edit User			
🗞 Mode	Search			
🔅 Device	User Capacity Info		User ID 12	
🖵 Display	Delete All Users	//	Name	
🧮 Log			Fingerprint None	
Back Horne	e cartes		Back Home	kave Save

- 1 After entering into the Admin Menu, select [User] > [Enroll User].
- 2 Enter the user ID and at least one of card information, password, and fingerprints.

Press [Save] button 👗 to complete user registration.

<b>User Info Items</b>	
Face	
User ID	
Name	
Fingerprint	
Card	
Password	
Administrator	
Duress Finger	
Bypass Card	
Individual Auth	
Access Group	

# **Enroll User**

### Face



Touch the photo area and then the builtin camera is turned on. On the LCD screen, your face will be seen. Press [Capture] to save the face image. The registered face image on the device will appear on the LCD display upon authentication and it can be exported to BioStar software for valid identification check.

### User ID



лм 07:59 Status

OWERTYULO

A S D F G H J K L

XCVBNM>Ente

Cancel

Name

ALEX

Enter the user ID and then press [OK]. The user ID can be specified within the range of 1~4294967295. When you are entering into a new enrollment menu, a user ID is automatically given by the terminal.

Enter the name and then press [OK]. You can use Korean characters, alphabets, numbers and special characters.

### Fingerprint



Select [Fingerprint] and then the fingerprint registration procedure starts. You can register 1 ~ 10 fingers. One user can generally use two fingers. A fingerprint should be entered twice for confirmation. Enter one fingerprint and then press [OK] in the window prompting confirmation and enter the next fingerprint. Press [Cancel] to end the input. The number of entered fingerprints is displayed under the menu.

	-	Do	not	register	an	injured	finger	or	one
		whe	ere th	ne finger	orint	is vague	Э.		
-									

Caution! - If the authentication success rate of a fingerprint is too low, delete the fingerprint and register a new fingerprint

**Note** *Please refer to [Chapter 1 > How to place a finger (p.15)].* 

[finger (p.15)].

#### 4 ADMIN MENU



The device reads the card ID contained in the card and registers the ID. When the card input screen appears, place the card into the card reader.

**Note** You must enter the user ID and at least one of card information/password/fingerprints to make a registration.



If this checkbox is checked, the user is registered as an administrator. If not, the user is registered as a general user.

### Duress Finger



Caution!

Duress Finger offers users a way of indication a duress situation, such as being forced to open a door. If the duress finger is presented, it allows access and simultaneously triggers the alarm or alert actions you specify. Duress finger can be set only when the user has entered two or more fingerprints in [fingerprint] menu. Select [Last finger] in the configuration window and then the last-entered fingerprint is used as a duress finger.

- Do not use the duress fingerprint in your general entrance
- Register a fingerprint which can be used without causing any suspicion

### Password



Enter the password and then press [OK]. A password should be entered twice for confirmation and composed of 4-~16digits of numbers. If you enter numbers less than 4 digits, an alarm message will be displayed and the password will not be registered.

#### 4 ADMIN MENU

#### Bypass Card



If required, select [Bypass Card]. Bypass card will allow the user to bypass regardless authentication mode of the device.

### Individual Authentication Mode

<sup>Jun 30</sup> лм 08:02	Status 🔻
Menu > User > Enroll User	_
Individual A	\uth
Card+Finger+Pin	
ID+Pin	~
ID+Finger	
ID+Finger/Pin	•
ID+Finger+Pin	$\sim$
🔹 Not use	-
	and a second
UK C	ancei
0	\$
Back Home	Save

If required, set the individual authentication mode. If a user is set as [Individual Authentication Mode], the selected individual authentication mode for the user is prior to the authentication mode for the terminal. The individual authentication mode works for the corresponding

authentication means only.

	To use the individual authentication mode, select
Note	[Menu] > [Mode] > [Operation] and check
	[Individual Auth Mode].

# Access Group

If required, set the access group. [Access Group] is set to whether the user can access it or not. You can select an access group from the access groups transferred from the BioStar software to the terminal.



- Press [Save] on the right-bottom side of the screen.
- A window indicating user enrollment completion appears. The User registration has completed.

# Edit/Delete User

Select [Menu] > [User] > [Edit User].



- In the user list, select a desired user.
- 2 Edit the user information and then press [Add]. This procedure is identical with that of new user registration.
- 3 The success screen is displayed.

To delete a specific user, follow the procedure below.



- 1 In the user list, check the checkbox of the user to be deleted.
- 2 Click the [Delete] icon at the right bottom of the screen.
- 3 In the window prompting confirmation of deletion, press [OK].

**Caution!** If you have deleted user data that is not stored in the BioStar database, the user data cannot be restored.

4 ADMIN MENU

# Search User

Select [Menu] > [User] > [Search], select the search method, and then press [OK].



### **Search by ID**



An ID search window appears. Enter the ID and then press [OK]. The user whose ID matches to the entered ID is searched.

### **Search by Name**



A name search window appears. Enter the name and then press [OK]. It is not necessary to enter all characters of the name. When you enter some starting characters of the name, all users who have the name starting with the entered characters are searched.

### Search by CSN



A card ID input window appears. Place the CSN card close to the card reader. The user who uses the card is searched.

# Checking the Registered User Info



- 1 Select [Menu] > [User] > [User Capacity Info].
- 2 You can check the number of registered users/user images/templates and the remaining capacity.

**Note**You can register up to 200,000 users (or 400,000**Note**fingerprint templates) and 5,000 user face images on the<br/>device.

# Deleting All Users

You can delete all users registered in the terminal.



- Select [Menu] > [User] > [Delete All Users].
- **2** Press [OK] in the window confirming the deletion and then all user data registered in the terminal is deleted.

**Caution!** If you have deleted user data that is not stored in the BioStar database, the user data cannot be restored.

# <Using Template Card>

# Registering a User to a Card

### Issuing a Card

When the terminal recognizes a template card, it reads the user information and template data from the card and requires users to place their fingerprint on the sensor for verification between live fingerprint and the fingerprint stored on the device.

The user information and fingerprints are not saved to the terminal but the template card only. Therefore, the user information must be separately managed.

To use the template card, select [Mode] > [Operation] > [Card Mode] and select [Use Template Card].

- 1 Select [Menu] > [User] > [Issue Card].
- 2 A registration window appears. Enter the user information.
- 3 Enter the User ID, Name, Fingerprint and Password.
- 4 Set the Administrator, Duress finger, Bypass card use and Access Group, if necessary.
- **5** Press [Issue] button at the right bottom and place the template card to the card reader to complete registration.



- The user registered as [Bypass Card] will be authenticated as Bypass regardless of the authentication mode of the terminal.
- **Note** [Access Group] is set to whether the user can access it or not. You can select an access group from the access groups transferred from the BioStar software to the terminal.

# Caution! You cannot use both the CSN Card and the Template Card simultaneously.

4 ADMIN MENU

# Formatting a Card

To use a card as a Template Card, all data saved in the card should be deleted.



- 1 Select [Menu] > [User] > [Format Card].
- 2 Place the Template Card to format to the card reader
- 3 A window confirming card format is displayed.

4 ADMIN MENU

# **Network Setup**

Set the network connection of BioStation T2. There are two network connections: direct connection that a BioStar client connects to a terminal and server connection that a terminal connects to the BioStar server.

# TCP/IP Setup

Set up TCP/IP for connecting the terminal and BioStar.



- Select [Menu] > [Network] > [TCP/IP].
- 2 LAN Type: Select the LAN type to be used for TCP/IP connection. (Values: Disabled/Ethernet/Wireless LAN)
- **3 Port:** Assigns the TCP/IP port for the terminal. The default value is '1470'.
- **4 Max Conn:** Sets the number of BioStar software that can be connected simultaneously. (Values: 1/4/8/16)
- 5 DHCP: Sets whether or not to use DHCP protocol.
- 6 **IP Address:** Enter the IP address when a fixed IP is used instead of DHCP protocol. If you don't know the IP address, please ask your network administrator.
- **7 Gateway:** Enter the gateway address when a fixed IP is used instead of DHCP protocol. If you don't know the gateway address, please ask your network administrator.
- 8 **Subnet:** Enter the subnet mask address when a fixed IP is used instead of DHCP protocol. If you don't know the subnet mask address, please ask your network administrator.

### Server Setup

The terminal can communicate with the BioStar software server or the server application developed by using SDK. In the [Server], configure the IP address and ports of the server to connect to the terminal.

<sup>Jun 30</sup> Thu Рм 02:27   Status ▼		Jun 30 Thu Рм 02:28	Status 🔻
Menu > Network		Menu > Network > Server	_
TCP/IP		Use Server	
Server		Server IP	Ø
^	× 1	1921100.0119	$\sim$
Serial		Port 1480	Ø
USB			
USB Memory			$\sim$
WLAN			
Back Home		Back	Anne Home

- 1 Select [Menu] > [Network] > [Server].
- 2 Use Server: Set up whether or not to use the server.
- 3 Server IP: Enter the server IP and then press [OK].
- **4 Port:** Enter the port of the server and then press [OK].
- 5 After setting up all of the items mentioned above, press [Back] or [Home] to apply the settings to the terminal.

# Serial Communication

Set the serial communication. The serial communication uses either of RS485 or RS232 and the connection type is classified to 'PC Connection' and 'SIO/Terminal Connection'.



- Select [Menu] > [User] > [Serial].
- **2 RS485-PC:** Set whether or not to use RS485 communication between the terminal and a PC and the network speed between the terminal and a PC.

(Values: 115200/57600/38400/19200/9600/Not used)

- **3 RS485-NET:** Set the RS485 communication with Secure I/O and other terminals. (Values: Not Used/Net-Slave/Net-Host)
  - Net-Slave: Sets the terminal as Slave.
  - Net-Host: Sets the terminal as Host.
- **RS232:** Set whether or not to use RS232 communication between the terminal and a PC and the network speed between the terminal and a PC. Since RS232 and RS485-PC use a physically-identical port, you can use RS232 only when RS485 is set to Not Used. (Values: Not Used/9600/19200/38400/57600/115200)

RS485 communication between terminals can be

**Note** *configured with one Host terminal and slave terminals up to 7. In this case, up to 4 Secure I/Os can be connected.* 

### USB



- Select [Menu] > [Network] > [USB].
- 2 USB: Check whether or not to permit USB connection to PC. (Mini USB)
- **3 USB Memory:** Check whether or not to permit USB memory connection. (USB A Type)

### USB Memory



- Select [Menu] > [Network] > [USB Memory].
- **2 Import:** In the window, select a terminal ID of which data will be imported and click [OK].
- **3 Export:** After touching [Export], wait until the export is completed.
- **4 Firmware Upgrade:** Select the version to upgrade and then press [OK].
- 5 After completing import and firmware upgrade, the terminal is rebooted.

	To use a USB memory, select [Menu] > [Network] >
Note	[USB] and check USB memory item and then you can
	enter into the [USB Memory] menu.

4 ADMIN MENU

### Wireless LAN

You can select one of 4 wireless LAN settings (Preset) saved in advance through the BioStar software.

To set the Preset, enter the SSID, encryption type, and encryption key through the BioStar software.



- 1 Select [Menu] > [Network] > [WLAN].
- 2 Select the Preset to be used for wireless LAN connection.

# **Authentication Mode**

You can authenticate users in the operation mode set for the specified time schedule. One time schedule used for setting the authentication mode can be selected among the time schedules set through the BioStar software. The maximum number of time schedules is 128.

# Finger Auth Mode

Thu PM 02:11 Status • Menu		Thu Рм 02:30 St Menu > Mode	tatus 🔻	Thu PM 02:30 Menu > Mode > Finger Auth	Status ▼ Mode
💄 User		Finger Auth Mode		Finger Always	
		Card Auth Mode		Finger+Pin Never	~
🗞 Mode		ID Auth Mode		T&A Key+Finger Never	
🔅 Device		Operation	•	T&A Key+Finger+Pin Never	
🖵 Display	17	T&A Mode	× //		$\sim$
Eg Log		T&A Event			
Back Home		Back Home		Back	Anne Home

- 1 Select [Menu] > [Mode] > [Finger Auth Mode].
- **2 Finger:** Authenticated by fingerprint only.
- **Finger + Pin:** Authenticated by entering the fingerprint and then the password.
- **1 T&A Key + Finger:** Authenticated by pressing the corresponding T&A event key and entering the fingerprint.
- **5 T&A Key + Finger + Pin:** Authenticated by pressing the corresponding T&A event key and entering the fingerprint and password.

# Card Auth Mode



- Select [Menu] > [Mode] > [Card Auth Mode].
- **2 Card Only:** Authenticated by card only. In this mode, the card type to be used for authentication must be specified on [Mode > Card Mode].
- 3 **Card + Pin:** Authenticated by placing the card into the reader and entering the password.
- **4 Card + Finger:** Authenticated by placing the card into the reader and entering the fingerprint.
- **5 Card + Finger/Pin:** Authenticated by placing the card into the reader and entering the password or a fingerprint.
- **6 Card + Finger + Pin:** Authenticated by placing the card into the reader and entering a fingerprint and the password.

# ID Auth Mode



- 1 Select [Menu] > [Mode] > [ID Auth Mode].
- 2 **ID + Pin:** Authenticated by entering the ID and then the password.
- **3 ID + Finger:** Authenticated by entering the ID and then the fingerprint.
- **ID + Finger/Pin:** Authenticated by entering the ID and then entering the password or a fingerprint.
- 5 **ID + Finger + Pin:** Authenticated by entering the ID, the fingerprint and then the password.

### Operation



- 1 Select [Menu] > [Mode] > [Operation].
- **2 Face Detection:** Set to use Face Detection or not. When face detection is checked, authentication is successfully made only when face detection is succeeded after card or password authentication.
- **3 Dual Authentication:** Set the Dual authentication mode. Dual Authentication needs consecutive authentications from two different users for high security. If the second authentication is not made within 15 seconds from the first authentication, the first authentication will become invalid and you have to do dual authentication again.
- **4 Card Mode:** Set the card type used on the terminal. (Values: Not Used/Use CSN/Use Template Card) The EM model supports CSN card authentication mode only.
  - CSN: A terminal reads the unique Card Serial Number (CSN) given to a card and then saves the number. When a card is placed close to the card sensor by the terminal, the terminal then reads the CSN and compares the CSN to the CSN saved in the terminal for identification purposes.

- Template Card: User information including user ID and other identification information is saved in the card. When a card is placed close to the card sensor by the terminal, the terminal then reads the user information from the card for identification purposes.
- **5 Server Matching:** Set to use Server Matching or not. If Server Matching is selected, authentication is based on the user data saved in the server, instead of in the terminal. If connection to the server is disconnected, authentication is based on the user data saved in the terminal without making any additional changes to the configuration. Server matching works only with BioStar SE (Standard Edition). Please refer to BioStar user guide for detail.
- 6 **Match Timeout (5/10/15/20/25/30):** Sets up the waiting time for Server Matching and Face Detection. In case there is no answer from the server during Matching Time or the face cannot be detected, the authentication will fail.
- 7 Individual Auth: Sets whether or not to use the Individual Authentication mode. You can set authentication mode by individual user. Individual authentication mode for the user is prior to the authentication mode for the terminal.

### T&A Mode

Set up the T&A mode to apply to the terminal.



- 1 Select [Menu] > [Mode] > [T&A Mode].
- 2 Press [T&A Mode] to set the mode. (Disabled/Manual/Auto/Manual Fix/Fixed)

	For more details on the T&A mode,
Note	see [Chapter 3. User Menu >2. T&A Mode > T&A Mode
	Setup (p.46)].

### T&A Event

BioStar software allows you to check automatic time and activation of T&A events with F1~F4 or the additional T&A events (EXT 01~12). T&A events can be set up through BioStar only. On the terminal, the events can only be checked.

<sup>Jun 30</sup> Thu Рм 02:30   Status ▼		<sup>Jun 30</sup> Thu Рм 02:32	Status 🔻
Menu > Mode		Menu > Mode > T&A Event	
Finger Auth Mode		F1 - Fixed(by device) In - Never	
Card Auth Mode		F2 Out - Never	^
ID Auth Mode		F3 In Duty - Never	•
Operation		F4 Out Duty - Never	•
T&A Mode		EXT1	$\sim$
T&A Event		EXT2	
Back Home	•	Back	A Home

<sup>1</sup> 2

Select [Menu] > [Mode] > [T&A Event].

You can check the settings through the BioStar software.

# Camera Event

When a camera event occurs, the camera will start recording when the event begins and then save the still image log. Camera events can be set up through BioStar only. On the terminal, the events can only be checked.

- Select [Menu] > [Mode] > [Camera Event].
- 2 You can check the settings through the BioStar software.
## **Device Setup**

### **Fingerprint Setting**

Select [Menu] > [Device] > [Fingerprint].



**Security Level (Normal/Secure/Most Secure):** The security level is determined by False Acceptance Ratio (FAR). FAR stands for a ratio of accepting unregistered fingerprints. The lower the FAR is, the higher the security is, however, FRR (False Reject Rate) gets higher so that the recognition ratio of the registered users gets lower.

For the general T&A management purposes, we recommend the Normal. However, if you need high access control and security, we recommend you to raise the security level from Moderate to Secure or Most Secure.

- 2 Fast Mode (Normal/Fast/Fastest/Auto): If 1:N Recognition Mode is used while hundreds of users are saved in the terminal, the recognition time may be too long. In this case, you can reduce the recognition time by setting the speed of 1:N recognition. At this time, FRR may be higher than before. [Auto] automatically determines the recognition speed according to the number of total fingerprint templates registered to the terminal.
- **3 View Image:** Check whether or not to display the fingerprint image on the screen. With this function, users can check the registered fingerprint image on the LCD screen and input the right fingerprint.
- **4 Sensitivity (0~7):** Set the sensitivity of the fingerprint scanner. At the high sensitivity, it is easier to enter fingerprints. However, at the low sensitivity, the quality of entered fingerprint images can be always high. For the general use, we recommend you to set the value to Max. If the terminal can be affected by direct sunlight, relieve the effect by lowering this value.
- **5** Scan Timeout(sec) (1~20): Set the fingerprint input time and then press [OK]. Authentication fails when the user does not enter the fingerprint within the specified time.
- **6 Fake Detect:** Check whether or not to run an examination to detect the fake fingerprint attack.
- 7 Template Type (Suprema/ISO 19794-2/ANSI 378): Set the template type and then press [OK].

**Note** *Generally, the default values are recommended.* 

### Door

Select [Menu] > [Device] > [Door].



- **Relay:** Select a relay to open the door on authentication. (Values: Not Used/ Internal Relay 0/ Internal Relay 1/ External Relay 0/ External Relay 1/ SIO0 Relay 0/ SIO0 Relay 1/ SIO1 Relay 0/ SIO1 Relay 1/ SIO2 Relay 0/ SIO2 Relay 1/ SIO3 Relay 0/ SIO3 Relay 1)
- **2 Driven by:** Set the event that triggers door opening and then press [OK].
  - All Events: The door is open regardless of the authentication event type.
  - Authentication: The door is open only for the general authentication events, not for the T&A events.
  - T&A Event: The door is open for the T&A events where the relay will be used.
  - Authentication + T&A Event: The door is open for the T&A events where the relay will be used among the general authentication and T&A authentication.
  - Disabled: The door is not open for all events including all general authentication events and all T&A events.

- **3 Duration (sec):** Sets up the time for which the relay keeps the door open after an event. The relay will close the door again after the time has elapsed.
- 4 RTE(Exit SW): Select the relay for the door switch and then press [OK]. (Values: Input 0/ Input 1/ Input 2/ Input 3/ SIO0 Input 0/ SIO0 Input 1/ SIO0 Input 2/ SIO0 Input 3/ SIO1 Input 0/ SIO1 Input 1/ SIO1 Input 2/ SIO1 Input 3/ SIO2 Input 0/ SIO2 Input 1/ SIO2 Input 2/ SIO2 Input 3/ SIO3 Input 0/ SIO3 Input 1/ SIO3 Input 2/ SIO3 Input 3)
- **5 RTE Type:** Select the door switch operation type and then press [OK]. (Values: N/O, N/C)
- **6 Door Sensor:** Select the detection mechanism for door opening and then press [OK]. (Values: Input 0/ Input 1/ Input 2/ Input 3/ SIO0 Input 0/ SIO0 Input 1/ SIO0 Input 2/ SIO0 Input 3/ SIO1 Input 0/ SIO1 Input 1/ SIO1 Input 2/ SIO1 Input 3/ SIO2 Input 0/ SIO2 Input 1/ SIO2 Input 2/ SIO2 Input 3/ SIO3 Input 0/ SIO3 Input 1/ SIO3 Input 2/ SIO3 Input 3)
- **7 Door Sensor Type:** Select the door sensor operation type and then press [OK]. (Values: N/O, N/C)
- 8 Held Open Period(sec): Set the duration of time for the alarm to go off after the door opens and then press [OK].
- **9 Unlock Time:** Set the time to keep the door forcibly unlocked. During the unlock time, the door is not closed. (Values: Not Used/ Always/ Auto IN/ Auto Out). The unlock time can be set through the BioStar only.
- **10** Lock Time: Set the time to keep the door forcibly locked and then press [OK]. (Not Used/ Always/ Auto IN/ Auto Out)

**Note** *Generally, the default values are recommended.* 

### Interphone Setting

Select [Menu] > [Device] > [Interphone].



After setting the interphone, you can make a call by pressing the Call key on the BioStation T2 terminal. The following screens show screens per interphone type.



Connecting

Analog Interphone

IP Interphone

- **Interphone:** Select an interphone to use and then press [OK]. (Not use/Analog Interphone/IP Interphone)
- 2 Video Server IP: If you have selected IP Interphone, enter the video server IP. If you don't know server IP, please ask your network administrator.
- **3 Video Server Port:** Enter the video server port. If you don't know server Port, please ask your network administrator.
- 4 VoIP Server IP: If you have selected IP Interphone, enter the VoIP server IP.
- **5 VoIP Phone Number:** If you have selected IP Interphone, enter the VoIP phone number.
- **6 VoIP Display Name:** If you have selected IP Interphone, enter the VoIP name.
- **7 VoIP Server ID:** Enter the VoIP server ID. You can use alphabets, numbers and special characters.
- **8 VoIP Server Password:** Enter the VoIP server password and then press [OK].
- **9 VoIP Mic Gain:** Adjust the volume of the VoIP microphone (0~10).
- **VoIP Speaker Gain:** Adjust the volume of the VoIP speaker (0~10).

	The only following videophone models are compatible with				
	BioStation 12.				
Note	- COMMAX / CAV-35N				
	– COMMAX / CAV-50H				
	– COMMAX / CAV-50P				

### Date & Time Setup

Set up the time displayed on the terminal. Set up the accurate time to receive accurate log data.

Select [Menu] > [Device] > [Date & Time].



- **Date (YYYY/MM/DD):** Enter the current date by using [<] and [>] and then press [OK].
- **2** Time (PM//hh/mm/ss): Enter the current time by using  $[\land]$  and  $[\lor]$  and then press [OK].
- **3 Time Sync:** You can use Time Sync in the server mode. The terminal's time will be synchronized with the server time. The time will be synchronized once every hour and only if the time difference between terminal and server is more than 5 seconds.

### Device Info

You can check the model name, device ID, H/W version, F/W version, kernel version, MAC and fingerprint module version. Select [Menu] > [Device] > [Device Info].



### Memory Info

Check the memory usage status. Select [Menu] > [Device] > [Memory Info].



## **Touchscreen Calibration**

Select [Menu] > [Device] > [Touchscreen Calibration].

- Press the cross mark on the screen. When the cross mark moves, follow it by touching with your finger on the screen.
- 2 After calibration is finished, the cross mark will soon disappear

### **Touchkeypad Calibration**

Adjusts the sensitivity of the bottom touch keys. As the setting value is smaller, the sensitivity is high. As the setting value is larger, the sensitivity is low.



- Select [Menu] > [Device] > [Touchkeypad Calibration].
- 2 Set sensitivity of each of F1~F4 keys and the Call key. (Value: 0~9)

**Note** *Generally, the default value is recommended. The factory default value is* [4].

### **Reset**

Reboots the BioStation T2 terminal.

- 1 Select [Menu] > [Device] > [Reset].
- 2 Press [OK] to reset the terminal.

### Factory Default

Initializes the BioStation T2 to the factory default.

- 1 Select [Menu] > [Device] > [Factory Default].
- 2 Press [OK] to reset all settings to the factory default value.

**Caution!** Please be aware that the factory default means that all wallpapers, sound effects, notices, etc. that you have downloaded from BioStar will be deleted. However, even if you execute factory default, the registered user data and log data will not be deleted.

4 ADMIN MENU

## **Display Setup**

### Select [Menu] > [Display].



	If [Notice] and [Slide Show] are selected, the logo screen			
	will be displayed for authentication or other operations			
	and one of the notice screen, the slide show screen, and			
	PDF screen will appear when the menu timeout has			
Note	passed (after 30 seconds if the menu timeout has been set			
	to Unlimited). When you touch the screen in the [Notice]			
	or [Slide Show] status, the LCD backlight will be turned			
	on if it is turned off. If the LCD backlight is already			
	turned on, the screen will be switched to the logo screen.			

- **Theme:** Select a theme for the screen background and then press [OK]. (Values: Theme 1/Theme 2/Theme 3/Theme 4)
- 2 Background: Select a background for the Standby screen and then press [OK]. (Values: Logo/Notice/Slide Show/PDF]
- **3 Voice Instruction:** Select whether or not to use the voice announcement. You can change pre-defined voice announcement by an event through BioStar Software.
- **4 Menu Timeout:** If no key is pressed during the selected timeframe, the display returns to main screen (Values: Infinite/10 sec/20 sec/30 sec)
- **5 Pop-Up Time:** Select how long the message will be displayed on the screen during authentication (Values: 0.5 sec/1 sec/2 sec/3 sec/4 sec/5 sec)
- **6 Backlight Timeout:** If no key is pressed during the allotted timeframe, the LCD backlight will be turned off (Values: Unlimited/10 sec/20 sec/30 sec/40 sec/50 sec/60 sec)
- **7 Volume (0~100%):** Select volume of the sound effects. 0% means that no sound will be emitted.
- 8 **Language:** Select the language displayed on the terminal and then press [OK]. You have to reboot the terminal to activate language changes.
- **9 Central Time Display:** Select whether or not the time and date will be displayed on the center of standby screen.
- **10 Date Display (MM/DD,DD/MM):** Select the date display format on the terminal and then press [OK]

4 ADMIN MENU

#### Log Log List рм 02:11 | Status 🗸 рм 02:39 Status 🔻 💄 User Log List **∃**₽ Network Log Search 🚵 Mode Delete All Log 🔅 Device 🖵 Display



Select [Menu] > [Log] > [Log List], then the list of logs will be displayed.

Select a desired log to view the details. 2

0

The still image log is marked 3

🧮 Log

1

0

рм 07:07 | Status 10091 USER Finger Identify OK In OK 0 

Event Log



Still Image Log

### Log Search



- Select [Menu] > [Log] > [Log Search].
- Select a desired item among Start Date, Start Time, End Date, 2 End Time, Event, T&A Event, and User ID and then press [Search].
- The result of searching logs is displayed. 3

### **Delete All Log**



- 1 Select [Menu] > [Log] > [Delete All Log].
- 2 Press [OK] to delete all saved logs.

### Log Info



- 1 Select [Menu] > [Log] > [Log Info].
- 2 Check the number of logs saved in the terminal and the remaining available capacity.

**Note** You can save up to 1,000,000 event logs and up to 5,000 still image logs.

HTTP://WWW.SUPREMAINC.COM

# 5 APPENDIX

**BioStation T2 User Guide** 

## **Product Specifications**

Item	Specifications					
Card Options	125KHz EM, 13.56MHz ISO14443 A/B (MIFARE)					
	Maximum Number of Users	200,000				
Capacity	Template Capacity	400,000(1:1), 20,000(1:N)				
	Log Capacity	Fingerprint: 1,000,000 / Still Image Log: 5,000				
	Communication Interface	Ethernet, WLAN, RS485 x 1ch, RS232/RS485(changeable) x 1ch, USB				
lucke of a se	Wiegand	IN&OUT (Switchable)				
Interface	TTL I/O	4 inputs				
	Built-in Relay	2				
	PoE	Yes				
	CPU	667Mhz RISC x 1, 533MHz DSP x 1				
	Memory	1GB flash, 256MB RAM				
	LCD Display	5.0 inch WVGA touchscreen				
	Fingerprint Sensor	Optical				
	Camera	Face detection & videophone				
Hardware	Audio	16 bit Hi-Fi voice & sound indication				
	Operating Temperature	-20°C ~ 50°C				
	Humidity	90%				
	Tamper	Switch				
	Input Voltage	12V DC				
	Dimensions	155 mm(W) x 155 mm(H) x 40 mm(D)				

# **Electrical Specification**

	Min. Value	Mean Value	Max. Value	Remark			
Power							
Voltage (V)	10.8	12	13.2	Use the power adapter which meets the specifications.			
Current (mA)	-		1500				
Switch Input							
VIH(V)	-	TBD	-				
VIL(V)	-	TBD					
Pull-up Resistance (Ω)	-	4.7K	-	The input ports are pulled up with 4.7 K $\Omega$ resistors.			
Wiegand Output							
VOH(V)	-	5	-				
VOL(V)	-	0.8	-				
Pull-up Resistance (Ω)	-	4.7K	-				
Relay							
Switching Capacity (A)	-	-	2 0.3	30V DC 125V AC			
Switching Power (resistive)	-	-	30W 37.5VA	DC AC			
Switching Voltage (V)	-	-	110 125	DC AC			

5 APPENDIX

## **FCC Rules**

### Caution

Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

### Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interface, and (2) this device must accept any interface received, including interference that may cause undesired operation.

### Information to User

This equipment has been tested and found to comply with the limit of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, user and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation; if this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more the following measures:

- 1. Reorient / Relocate the receiving antenna.
- 2. Increase the separation between the equipment and receiver.
- 3. Connect the equipment into an outlet on a circuit difference from that to which the receiver is connected.
- 4. Consult the dealer or an experienced radio/TV technician for help

## **Font License**

Copyright (c) 2010, NHN Corporation (http://www.nhncorp.com), with Reserved Font Name Nanum, Naver NanumGothic, Naver NanumGothic, Naver NanumGothic, Naver NanumMyeongjo.

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

### SIL OPEN FONT LICENSE

Version 1.1 - 26 February 2007

### PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves.

The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works.

The fonts and derivatives, however, cannot be released under any other type of license.

The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

### DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s). "Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting ? in part or in whole ? any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

### **PERMISSION & CONDITIONS**

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

### TERMINATION

This license becomes null and void if any of the above conditions are not met.

### DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.





## Suprema Inc.

16F Parkview Office Tower, Jeongja-dong, Bundang-gu Seongnam, Gyeonggi, Korea 463-863 TEL : 82 31 783 4502 FAX : 82 31 783 4503

Customer Support : support@supremainc.com

Website : www.supremainc.com

*The specifications and functions of BioStation T2 are subject to change without prior notice for continuous function or quality improvement. For more information on the product, contact Suprema Inc.*